REMARKS

By the above amendment, applicants have amended claims to define the invention more particularly and distinctly so as to overcome the technical rejections and define the invention patentable over the prior art. In addition, applicants thank the Examiner for the clear and understandable Office Action.

The Rejection of Claims 1, 6-8, 10-12, 14-19 and 20 Under 35 USC 103 (a) Overcome

The last O.A. rejected Claims 1, 6-8, 10-12, 14-19 and 20 for being unpatentable over Martherus et al (US Pub No. 2002/0112155), and in view of Guski et al (US Patent No. 5,592,553).

Claim 1

Claim 1 has been reexamined over the combination of referenced prior-art. Applicants request reconsideration of this rejection for the following reasons:

1) As explained in the following, the method and system described in Claim 1 solves a different problem and produces unexpected results. In addition, the prior-art references produce an inoperative combination or combination which does not meet Claim 1.

   The last O.A. notes (p. 4) that it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Guski into the teaching of Martherus to generate one-time identity codes. This modification would be obvious because one of ordinary skill in the art would be motivated to prevent unauthorized access to system resources by using the intercepted passwords together with nonsecret information as a user ID [Guski, col. 1 lines 25-28].

From Martherus's teaching, we learn that the main embodiment of the system is to use an Access System to authenticate a user for multiple domains in a network system, i.e.,

Martherus (paragraph 73 lines 1-4):
"FIG. 1 depicts an Access System which provides identity management and access management for a network. In general, an Access System manages access to resources available to a network.",

and Martherus (paragraph 11 lines 1-3):
"The present invention, roughly described, provides for a system capable of authenticating a user for a plurality of domains in a network-based system.".

Martherus's Access System does not function as an authentication authority as described in Claim 1. Martherus's Access System contains both user authentication and user authorization to access available network resources at a granular level for a plurality of network domains in an affiliated E-business system, i.e.

Martherus (paragraph 73 lines 3-9):
"In general, an Access System manages access to resources available to a network. The identity management portion of the Access System (hereinafter "the Identity Management System") manages end user identity profiles, while the access management portion of the Access System (hereinafter "the Access Management") provides security for resources across one or more web servers.",

and Martherus (paragraph 7 lines 1-9):
"To meet these challenges, an E-business host company needs a web access management solution that delivers the ability to effectively

secure and manage all the various network-based interactions. A system should accommodate all participants involved with the E-business, whether they are local or remote. It must also be able to distinguish between the E-business' employees and all the users who are affiliated with the E-business host's customers, suppliers and/or partners.".

In contrast, the authentication authority described in Claim 1 is an autonomous system residing on the Internet to authenticate a plurality of user identities to a plurality of network domains. Furthermore, the authentication authority described in Claim 1 only provides user authentication and does not authorize the access to any user resources of an E-business host company or E-business host affiliates on any network domain. Moreover, the authentication authority does not authorize access to any user resources on any network domain.

To further the discussion, applicants recognize that Martherus's Access System consists of Access Server, Web Gate, and Access Manager, i.e.,

Martherus (paragraph 83 lines 1-3):
"The Access Management System includes Access Server 34, Web Gate 28, Web Gate 30 (if enabled), and Access Manager 40.".

The last O.A. suggests (p.2) that the function of Martherus's Access Server is equivalent to the authentication authority, i.e.,

Martherus (paragraph 83 lines 3-4):
"Access Server 34 provides authentication, authorization, and auditing (logging) services.".

The last O.A. also suggests (p.2) that the function of Martherus's Web Gate is equivalent to the gateway authority for Web Gate communicating with and forwarding requests to Access Server, i.e.,

Martherus (paragraph 83 lines 7-8):
"Web Gate 28 acts as an interface between Web Server 18 and Access Server 34.",

Martherus (paragraph 80 lines 2-3):
"Web Gate 28 is a plug-in to Web Server 18. Web Gate 28 communicates with Access Server 34.",

and Martherus (paragraph 189 lines 16-17):
"Web Gate 28 transmits a flag with all POST requests forwarded to Access Server 34".

The last O.A. also suggests (p.2) that the function of Martherus's Web Browser is equivalent to the authentication client, i.e.,

Martherus (paragraph 74 lines 7-8):
"web browser 12 and 14 are standard web browsers known in the art running on any suitable type of computer. FIG. 1 depicts web browser 12 and 14 communicating with Web Server 24 and Administration Server 20 using HTTP over the Internet; ...".

The last O.A. also suggests (p.3) that the function of Martherus's Web Server is equivalent to the authentication handler to protect resources of business entities, i.e.,

Martherus (paragraph 75 lines 1-3):

"Web Server 18 is a standard Web Server known in the art and provides an end user with access to various resources via Internet 16.".

The last O.A. also suggests (p.3) that the method to process user's authentication requests among Martherus's Web Browser, Web Server, Access Server, and Web Gate is equivalent to that among authentication client, authentication handler, authentication authority, and gateway authority, i.e.,

Martherus (paragraph 88 lines 10-35):
"The user's browser sends the URL as the part of an HTTP request to Web Server 18. Web Gate 28 intercepts the request. If the end user has not already been authenticated, Web Gate 28 causes Web Server 18 to issue a challenge to the browser for log-on information. The received log-on information is then passed back to Web Server 18 and on to Web Gate 28. Web Gate 28 in turn makes an authentication request to Access Server 34, which determines whether the user's supplied log-on information is authentic or not. Access Server 34 performs the authentication by accessing attributes of the user's profile and the resource's authentication criteria stored on Directory Server 36. If the user's supplied log-on information satisfies the authentication criteria, the process flows as described below; otherwise, the end user is notified that access to the requested resource is denied and the process halts. After authenticating the user, Web Gate 28 queries Access Server 34 about whether the user is authorized to access the resource requested. Access Server 34 in turn queries Directory Server 36 for the appropriate authorization criteria for the requested resource. Access Server 34 retrieves the authorization criteria for the resource and, based on that authorization criteria, Access Server 34 answers Web Gate 28's

authorization query. If the user is authorized, the user is granted access to the resource; otherwise, the user's request is denied.".

The last O.A. also suggests (p.3) that the media for Martherus's system to authenticate user is similar to that described by applicants' invention, i.e.,

Martherus (paragraph 13 lines 10-12):
"Hardware that can be used for the present invention includes computers, handheld devices, telephones (e.g. cellar, Internet enabled, etc.), etc.".

As a result, applicants system should be very similar to that of Martherus's system. Moreover, as pointed by the last O.A. (p. 4), Martherus does not use an end-user device to generate the one-time identity codes. Thus, the last O.A. concludes that in view of Guski's teaching about using one-time identity codes, applicants' invention would have been obvious.

By a closer examination of Martherus's system, applicants found that Martherus's system is not designed nor operates the same as applicants' invention. Although Martherus's system allows the user authentication across multiple domains, this system is not an authentication authority as defined by applicants' invention. Instead, Martherus's system is designed to provide user access and authorization to multiple domain resources and operates using single sign-on authentication i.e.,

Martherus (paragraph 266 lines 1-3);
"In another embodiment, "affiliate" Web Gates are installed on remote Web Servers to provide single sign-on authentication across multiple organizations.",

and Martherus (Abstract lines 1-3):

"The present invention authenticates a user for multiple resources distributed across multiple domains through the performance of a single authentication.".

It is applicants' opinion that Martherus's system has an inherent security risk from the single sign-on authentication design. Specifically, if an imposter compromises the user login of single sign-on authentication made available from a Web Gate, Access Server, and Directory Server in one domain, then not only is user data in that domain at risk of compromise, but so is all user data distributed across multiple domains and allowed access from that single login. In contrast, applicants' invention does not provide a single sign-on authentication solution and is designed with the intention to decrease the security risk of user identity compromise with one-time identity codes. To access multiple domains in applicants' invention, the user needs to sign-on and authenticate multiple times. However, the user in applicants' invention generates one-time identity codes from a single authentication device with a single registration to a single authentication authority. Applicants' invention provides convenience and strong security for a user to manage his/her digital identity and authentication to multiple network domains accessible from the Internet.

Despite some functional similarities between Martherus's system and applicants' system, major design differences exist. For example, Martherus's Web Gate and Access Server are behind the Web Server and two firewalls, i.e.,

Martherus (paragraph 75 lines 3-6):
"In one embodiment, there is a first firewall (not shown) connected between Internet 16 and Web Server 18, a second firewall (not shown) connected between Web Server 18 and Access Server 34.".

Therefore, Martherus's Web Gate and Access Server residing behind two firewalls are not designed to be Internet accessible by the user. In contrast, the gateway authority and authentication authority of applicants' invention are positioned specifically for the user to access from the Internet. Applicants' web architecture differs greatly from the Martherus's system since it is not designed to provide a single sign-on authentication solution. Instead, the web architecture of applicants' invention is designed to provide a global identity authentication or verification solution for Internet users to sign-on and access multiple web sites with one-time identity codes that are generated by a single authentication device.

As a result, the combination of Martherus and Guski's teaching will produce a system that is inoperative for authenticating a user with one-time identity codes as described in Claim 1. To produce a workable and secure system, a significant modification of Martherus's teaching is necessary. Thus, Claim 1 is unobvious and patentable over the referenced prior-art.

2) The method and system described in Claim 1 effectively deals with an unsolved need and produces Synergism.

Phishing schemes have become a serious hazard for Internet users. Internet users may be tricked into disclosing their username or password information when attempting to access a fraudulent phishing web site appearing to resemble the intended web site. Without knowing the authenticity of the web site, the Internet user may begin to enter username and password information for the fraudulent web site account login. Indeed, this Internet user will not actually access the intended web site. However, the Internet user may have already disclosed the username and password information to the phishing web site. Thus, the Internet user has

become a victim of identity theft. The stolen information may be quickly used by the phishing thief to access the intended web site and compromise the user's confidential information and successfully execute financial transactions with the Internet user's stolen identity. The financial services industry on the Internet has been a favorite target of phishing attacks.

Consequently, the Federal Financial Institutions Examination Council (FFIEC), a U.S. financial services oversight council composed of members including the Federal Reserve Board, Federal Deposit Insurance Corporation, and National Credit Union Administration, revised its guidelines in October of 2005 recommending that all financial services on the Internet strengthen their access controls for authentication by the end of 2006.

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties.

The FFIEC will soon examine Internet financial services in 2006 to determine if access controls for authentication have been strengthened and that other factors including the use of one-time passwords to supplement single-factor authentication systems have been implemented.

A variety of solutions in the marketplace offer stronger access controls for authentication via one-time passwords that may be considered by financial services. Yet, most of these solutions create other impractical implementation issues for the online financial service that may further delay or even prevent their customers from having strong authentication readily available using one-time passwords to mitigate the growing threat of phishing attacks in 2006. For example, RSA Security, the market leader in providing one-time password hardware tokens, requires a closed system

of network domains to establish the two-factor authentication system. The RSA solution would require the financial service customer to maintain a separate token for each one-time password authentication system since the RSA implementation is a closed system. This design creates a burden for Internet users, and it would not be uncommon for an Internet user to carry several one-time password devices for strong authentication of financial services. For example, the Internet user may have his checking and savings account with one bank, money market and brokerage services with another financial service, and mortgage banking with another. Each of these services would require a separate one-time password token for each service. Thus, the Internet user in the previous example would be burdened to carry three separate devices implemented by financial services in order to meet FFIEC compliance guidelines. In addition, other Internet web sites will inevitably require stronger authentication measures that potentially include one-time passwords due the growing menace from phishing on a global scale and include: commercial web sites such as online auction houses, retail consumer web sites, or government Internet services from the IRS or Social Security Administration. Hence, the global demand for stronger authentication via one-time passwords further complicates the multiple token burdens for the Internet user.

Another problem arising from the RSA hardware token one-time password solution is the additional overhead required to service the RSA token. For example, the financial service would not only need to buy tokens to issue to their customers, but also need to purchase additional servers to validate these one-time password tokens, and find a means to support, distribute, and maintain the authentication needs for the life of the tokens. This type of implementation is complex and does not have the simple and elegant design met by the applicants' invention. It is likely that financial services have been reluctant to embrace the hardware token solution in the past for its sheer complexity to implement and burden to the customer.

Applicants' invention effectively deals with the complications arising from multiple one-time password hardware tokens through its simple and elegant means to access multiple web sites with a single one-time password authentication device. Furthermore, applicants' invention may be quickly implemented by financial services to meet FFIEC guidelines since the authentication authority and authentication gateway reside on the Internet and are made available without requiring major infrastructure changes in the financial services authentication system to begin using stronger authentication with one-time passwords. Moreover, the client authentication device is not a hardware token with a limited lifetime and may be in the form of a variety of mobile devices that the financial service is not required to distribute and maintain.

Applicants' invention is designed to resolve the above mentioned problems. The idea of using one-time identity codes and developing a global authentication authority system which comprises four distinctive components (i.e., authentication authority, authentication handler, authentication gateway, and authentication client), and use Web services to connect them is simple and elegant. It provides security, convenience, and scalability. Because of this simple and elegant design, the impact to the Internet financial services industry can be tremendous. For example, financial services may implement applicants' solution to satisfy the guidelines set by the FFIEC, so vast numbers of online banking Internet users can have a secure way to protect their bank accounts without the burden of multiple tokens and effectively deal with an unsolved need for stronger authentication. In addition, the implication of synergism is obvious because this invention is designed to scale globally on the Internet, and may apply to all forms of Internet services including financial, consumer retail, government, and other web sites that seek stronger authentication using one-time passwords.

3) The proto-typed system described in Claim 1 has been developed and tested by applicants' for commercial use. The invented authentication authority Web services are available over the Internet at www.globalkey.biz. Enhanced security functions to the GlobalKey service to combat phishing continue to be developed and deployed for commercial operation on the web site.

Claim 6

As explained in the remarks of Claim 1 above, Martherus's Access Server and Web Gate are placed behind two firewalls inside the organization's Intranet. This design is very different from that of the authentication authority and gateway authority as described in applicants' invention. This invention utilizes a new principle of operation. Thus, Claim 6 is unobvious and patentable over the referenced prior-art.

Claim 7

Claim 7 is amended to include "for the Internet user" for clarity. The registered user of Martherus's Access Server is either its Intranet domain user, or its affiliated E-business Extranet domain user. One has to be authorized to access domain resources to become a registered user of Martherus's Access Server. The user registration and the identity management are highly controlled by the Access Server, i.e.,

Martherus (paragraph 6 lines 3-6):
"For example, businesses need to securely provide access to business applications and content to users they deem authorized.",

Martherus (paragraph 7 lines 1-9):
"To meet these challenges, an E-business host company needs a web access management solution that delivers the ability to effectively secure and

manage all the various network-based interactions. A system should accommodate all participants involved with the E-business, whether they are local or remote. It must also be able to distinguish between the E-business' employees and all the users who are affiliated with the E-business host's customers, suppliers and/or partners.",

Martherus (paragraph 85 lines 1-5):
"User Manager 38 provides a user interface for administrators to use, establish and/or manage identity profiles. An identity profile (also called a user profile or user identity profile) is a set of information associated with a particular user.",

and Martherus (paragraph 99 lines 9-10):
"Revoked user list 108 identifies users previously (but no longer) allowed access to resources on their system.".

In contrast, the registered user of the authentication authority can be any person with a digital identity on the Internet. The authentication authority provides a global identity authentication or identity verification one-time password solution to global set of registered users. In addition, the authentication authority does not have any control over the business authorization of accessed resources. The authentication authority leaves the authorization responsibility to the individual business entity. Furthermore, the authentication authority does not play any role in managing a user's digital identities. The user has the ability to control and manage his/her digital identities. This invention utilizes a new principle of operation. Thus, Claim 7 is unobvious and patentable over the referenced prior-art.

Claim 8

As explained in the remarks of Claim 1, 6, and 7 above, applicants' invention utilizes a new principle of operation to register, manage, and authenticate a user's digital identity. Martherus's system is a highly centralized enterprise system to control not only the authentication but also the authorization processes. In contrast, the authentication authority is a user controlled autonomous system. The main function of the authentication authority is to assist business entities to verify or authenticate a user's self managed digital identity with one-time passwords. Therefore, it would not have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Guski into the teaching of Martherus to generate one-time identity codes.

The last O.A. notes (p.5) that in view of Guski (col.1 lines 25-28), i.e., **"Such person may thereafter attempt to gain unauthorized access to system resources by using the intercepted passwords together with such nonsecret information as a user ID which may also have been intercepted.",**

the modification would be obvious because one of ordinary skill in the art would be motivated to prevent unauthorized access to system resources by using the intercepted passwords together with non-secret information as a user ID.

It is applicants' opinion that the combination of Martherus and Guski's teaching would produce an authentication system often implemented in the current marketplace. It is a system that applies strong authentication using one-time passwords for access to a single authentication and authorization system for the purpose of sharing authorized resources across multiple networked Extranet domains from affiliated E-business enterprise servers. Therefore, the combination of Martherus and Guski's teaching will not produce an operative global authentication authority system as described in Claim 1. Thus, Claim 8 is unobvious and patentable over the referenced prior-art.

Claim 10

Martherus (paragraph 88 lines 32-34) teaches:

"Access Server 34 answers Web Gate 28's authorization query. If the user is authorized, the user is granted access to the resource;".

The procedure to grant authorization to a resource is the hallmark of Martherus's system. Furthermore, as explained in the remarks of Claims 1, 6, and 8 above, Martherus's system is a centrally controlled enterprise system. The communication among Web Server, Web Gate, and Access Server is on the Intranet network of an internal enterprise environment. In contrast, the communication among authentication authority, gateway authority, and authentication handler of applicants' invention is on the external Internet environment using Web services technology, and the use of Web services is foreign to Martherus.

The use of Web services makes the implementation of the authentication handler very easy. As a result, web site owners are more likely to implement the authentication handler and subscribe to a global authentication authority system for stronger authentication of their Internet end-users. Thus, it is obvious that this global authentication authority system of applicants' invention is far superior to that of the centrally controlled enterprise system as described by Martherus. This superiority of the global design will produce unexpected results.

Claim 11

The last O.A. notes (p.6) that **"Guski teaches that generates synchronization codes and conduct synchronization.".** The cited paragraph (col.3 lines 28-32) is listed as the following:

"The authenticator compares the regenerated time-dependent information with reference time-dependent information and grants access to a resource in

accordance with the comparison of the regenerated time-dependent information with the reference time-dependent information."

Upon closer examination, it is applicants' opinion that Guski describes a time synchronization method to recover the time-dependent information and the authentication parameter from the password. The recovering process involves the use of the inverse function to decrypt the password using two predetermined transformation functions (first and second transformation), i.e.,

Guski (col. 3 lines 20-27):
"The authenticator regenerates the time-dependent information from the password by (1) regenerating the authentication parameter from the password presented to the authenticator using the inverse of the second transformation and then (2) regenerating the time-dependent information from the authentication parameter using the inverse of the first transformation.".

The purpose of conducting synchronization between the authentication client and authentication authority in applicants' invention is to compute the non-predictable number without transmitting user private identities over any communication channel. Thus, the referenced art lacks any suggestion that the combination of Martherus and Guski can produce an operative system as described in Claim 11. This proves that Claim 11 is unobvious.

Claim 12

The last O.A. notes (p.7) that Guski teaches how to incorporate user identity information to generate a one-time password, i.e.,

Guski (col. 7 lines 45-49):
"FIGS. 4 and 5 show the procedure used by the password generator 300 (FIG. 3) to generate a one-time password 310 as a function of a secret

quantity (the host signon key 306), nonsecret information 302 and 304 identifying the user and the host application, and time/data information 308."

Applicants agree that the synchronization described in Claim 12 also uses similar user attributes as the input information to generate the one-time password. However, the operator to process that information is entirely different. Guski uses bit level DES and XOR operators (Guski FIG. 4), while Claim 12 of this invention uses byte level hashing, power and modular math operators. Guski's process is reversible, while that of applicants' is not reversible. Therefore, the referenced art does not contain any suggestion that the computation of the synchronization code could meet the requirement as described in Claim 12. This is the evidence that Claim 12 is not obvious.

Claim 14

The confirmation codes described in Claim 14 are used to verify the success of synchronization. As explained in the remark of Claim 11, Guski describes a method and process to recover the time-dependent information and the authentication parameter from the password. The purpose of having the time-dependent information is to resolve a performance issue, i.e.,

Guski (col. 2 lines 10-25):

"The system described in the above-identified copending application has a performance problem at the authenticating end, since the only way in that system to ensure that the incoming one-time passwords are valid and not intrusion attempts is to generate a corresponding one-time password and compare the incoming one-time password with the generated one. The generation of one-time passwords requires repeated uses of the DES encryption procedure, which is computationally intensive. This problem is further compounded because the input to the one-time password generation process involves time information as one of the input variables. Because no

two computer clocks are ever set exactly the same and a delay can occur while the one-time password is in transit, multiple passes through the procedure for various time values centered about the current clock value of the validating computer are necessary."

Therefore, the referenced art does not contain any suggestion that the computation of the confirmation code could meet the requirement as described in Claim 14. Guski's main point is to develop a system to recover the clock time information. It is applicants' opinion that Guski may not have a secure way for handling the one-time password generation, because the time-dependent information can be regenerated by the decryption which is a reversible process. It is obvious that Claim 14 solves a different problem than that of Guski. This demonstrates that Claim 14 is unobvious.

Claim 15

The following is a procedure that Guski describes to generate a one-time password, i.e.,

Guski (col. 2 line 63 to col. 3 line 10):

"In one aspect, the present invention contemplates an authentication system in which an authentication parameter (AP) is generated as a function of time-dependent information, preferably time-of-day (TOD) information, using a predetermined first transformation, the predetermined first transformation having an inverse transformation such that the time-dependent information may be regenerated from the authentication parameter using the inverse transformation. A time-dependent password comprising a character string, preferably an alphanumeric character string, is generated from the authentication parameter using a predetermined second transformation, the predetermined second transformation having an inverse transformation such that the authentication parameter may be regenerated from the password using the inverse transformation.".

Applicants summarize the above process as the following.

1. The one-time password is generated from the authentication parameter using a predetermined second transformation function which has an associated inverse function. This means that the one-time password is generated by encrypting the authentication parameter.
2. The authentication parameter is generated from time-dependent information using a predetermined first transformation function which also has an associated inverse function. This also means that the authentication parameter is generated by encrypting the time-dependent information.
3. The time-dependent information is composed of time-of-day clock information.

These two sets of encrypting processes can be clearly seen in Guski's FIG. 4 which indicates that the time-of-day information is processed by two sets of DES and XOR operations.

In contrast, the generation of one-time identity codes described in Claim 15 does not involve any encryption or decryption process. Instead, it uses a Diffie-Hellman type of algorithms, which involves the use of power and modular math operators. Furthermore, there is no one-time identity code related information in the form of encrypted or unencrypted messages being transmitted from the authentication client to the authentication authority in applicants' invention.

Therefore, the referenced art does not contain any suggestion that the computation of the one-time identity code could meet the requirement as described in Claim 15. This demonstrates that Claim 15 is unobvious.

Claim 16

As discussed in the remarks of Claims 12 and 15, the referenced art does not contain any suggestion that the computation of the non-predictable sequence

number could meet the requirement as described in Claim 16. This demonstrates that Claim 16 is unobvious.

Claim 17

The user private identities (user profile) described in Martherus's system is for access control and authorization purpose, i.e.,

Martherus (paragraph 88 lines 1-7):
"With the system of FIG. 1 deployed, Web Server 18 (enabled by Web Gate 28, Access Server 34, and Directory Server 36) can make informed decisions based on default and/or specific rules about whether to return requested resources to an end user. The rules are evaluated based on the end user's profile, which is managed by the Identity Management System.".

The shared secret information used in Martherus's system is for the encrypting of cookies, i.e.,

Martherus (paragraph 99 lines 11-15):
"Shared secret(s) 110 are keys stored on Directory Server 36 used for encrypting cookies set on browsers 12 or 14 after a successful user authentication. Shared secret(s) (keys) 110 can change as often as desired by an administrator.".

In contrast, applicants' invention incorporates the user private identities information and the user's secret information only for the purpose of computing the synchronization code and the non-predictable sequence number. These two numbers comprise the input to generate one-time identity codes. Thus, the referenced Martherus art does not contain any suggestion that could meet the requirement as described in Claims 12, 16, and 17.

The user private identities used in Guski is for the computation of the one-time password, i.e.,

Guski (col. 6 lines 27-34):
"The requesting node machine 102 also has memory locations for storing a user ID (UID) 302 identifying the user, an application ID (AID) 304 identifying the host application being accessed, a signon key (K) 306 used as a key for the encryptions to be described, and a time/date value (T) 308. As indicated in FIG. 3, values 302-308 provide inputs to the password generator 300.".

Thus, Guski's one-time password is generated by using UID, AID, and T as the input information. It may appear that Guski's one-time password generation is similar to that described in Claims 12 and 16. However, as explained in the remark of Claim 15 above, Guski's one-time password is generated from two steps of encryption process. Thus, the user private identity information is inherently embedded in the one-time password. This result is not a desired secure approach. In contrast, the private identity information described in Claim 17 is not transported from the authentication client to the authentication authority by any means. Therefore, because of this one-time password high security consideration, applicants' invention is a superior system which can produce unexpected results.

Claim 18

The last O.A. notes (p. 8) that a handheld device is used in Martherus's invention, i.e.,

Martherus (paragraph 13 lines 10-12):
"Hardware that can be used for the present invention includes computers, handheld devices, telephones (e.g. cellular, Internet enabled, etc.), etc."

Strangely, paragraph 13 lines 10-12 is the only place that Martherus references the handheld device in the patent application. There is no further explanation about what the handheld device is used for in the patent. Clearly, the use of the one-time password or one-time identity codes is foreign to Martherus. Thus, it is suspected that Martherus does not use the handheld device to generate any password. In contrast, applicants' invention uses the handheld device to generate one-time identity codes. Thus, the referenced Martherus art does not contain any suggestion that could meet the requirement as described in Claim 18.

Claim 19

The use of Web services technology is foreign to Martherus. Web services technology makes the implementation of the authentication handler very easy. As a result, more web site owners will adopt the authentication handler and subscribe to a global authentication authority system for stronger authentication of their Internet users. Meanwhile, as more Internet web sites subscribe and embrace this global authentication authority system, more Internet users will choose to register with subscribed web sites that offer the global authentication authority because of the convenience of only having to carry a single client authentication device to generate the one-time identity codes for access to a plurality of web sites. Thus, the use of Web services technology can produce unexpected results.

Claim 20

As explained in the remarks of Claim 1 above, the method to process a user's authentication requests among Martherus's Web Browser, Web Server, Access Server, and Web Gate is different from the authentication client, authentication handler, authentication authority, and gateway authority. In addition, the use of Web services technology is foreign to Martherus. As explained in the remarks of Claim 19, the use of Web services technology can produce unexpected results.

Moreover, as explained in the remarks of Claim 1, there are web architecture differences between applicants' invention and that of Martherus's system. These

web architecture design differences are significant since applicants' invention provides a global identity authentication or identity verification solution for the Internet user to sign-on and access multiple web sites, while that of Martherus's provides a single sign-on authentication system for the purpose of sharing authorized resources over an Intranet and Extranet across multiple network domains among trusted enterprise servers. It is obvious that Claim 20 solves a different problem than that of Martherus. This demonstrates that Claim 20 is unobvious.

The Rejection of Claims 2, 3, 4 and 5 Under 35 USC 103 (a) Overcome

The last O.A. rejected Claims 2, 3, 4 and 5 for being unpatentable over Martherus et al (US Pub No. 2002/0112155), Guski et al (US Patent No. 5,592,553), and Brown et al (US Pub No, 2004/0199636 L. Brown).

Claim 2

The last O.A. notes (p.9) that the combination of Martherus, Guski, and L. Brown would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of L. Brown into the teaching of Martherus and Guski that use Web services to publish and discover the information.

L. Brown gives a teaching of Web services fundamentals, i.e.,

L.Brown (paragraph 25):

"The nature of Web services make them natural components in a service-oriented architecture. A typical service-oriented architecture is shown in FIG. 1. Service providers 11 host a network accessible software module. A service provider defines a service description for a Web service and publishes it to a service registry 13, as depicted by arrow 17. A service requester 15 at a

client computer uses a find operation, represented by arrow 19, to retrieve the service description from the registry 13 and uses the service description to bind with the service provider, as represented by connector 21, and to invoke or interact with the Web service implementation.".

Applicants' invention recognizes the importance of adopting the Web services technology and develops a global authentication system based on this technology. Thus, Claims 2, 3, 4, and 5 of this invention addresses the use of Web services to provide authentication authority services. The use of Web services in the applicants' system can produce unexpected and synergetic results, because the use of Web services technology can lead to an easy integration of the global authentication authority system. Easy integration will further lead to the prevalent adoption and use of the authentication authority system.

As explained in the remarks of Claim 1, Martherus's Access Server and Web Gate are placed behind two firewalls inside the organization's Intranet. This design is very different from that of the authentication authority and gateway authority as described in applicants' invention. Thus, there is a vast architecture difference between Martherus and applicants' invention. Martherus's system is a single sign-on authentication solution, while applicants' system is a global identity authentication or identity verification solution for the user to sign-on and access multiple web sites using one-time identity codes that are generated by a single authentication device. The reason that applicants' invention can achieve the global solution objective is due to the use of Web services technology.

Is it even possible for the Martherus's system to be modified to adopt Web services technology? It seems very unlikely. The fundamental requirement of providing Web services is that the services provided must be accessible from a server residing on the Internet. Martherus's Access Server and Web Gate are placed in a protected and controlled Intranet environment that cannot be accessed from the Internet. It is obvious that it requires a major architecture change for

Martherus's system to utilize Web services technology. If there is such a change, the function for providing access control and authorization intended by Martherus's system as originally designed may no longer operate successfully, since the access control to provide authorization to shared resources would be protected behind an Intranet. Web services technology would not allow the user access to these resources since the servers providing authorization to the shared resources would not be available on the Internet, and a single-sign on solution would not offer any advantage to the Internet user since it may only authenticate an identity for enterprise services in a closed system to the Internet. Hence, Web services modifications to Martherus's single sign-on authentication solution would not be sufficient to allow the user to authenticate with multiple web sites as described in applicants' invention. Moreover, this architecture change to Web services may render the use of the authentication cookie as unnecessary. This may result in the failure to provide the single sign-on solution itself that Martherus champions.

Thus, it is applicants' opinion that the combination of Martherus, Guski, and L. Brown's teaching will not produce a system that is operative for authenticating a user with one-time identity codes as described in Claim 1. This proves that applicants' system is unobvious.

Claim 3

The last O.A. notes (p.10) that L. Brown's teaching describes the use of WSDL and UDDI. The last O.A. suggests that the combination of Martherus, Guski, and L. Brown's teaching would have been obvious.

The same reason explained in the remark of Claim 2 can be used to prove that Claim 3 is not obvious. It is improbable for Martherus's system to use WSDL and UDDI, because it requires a significant architecture change. Thus, the combination of referenced arts will not produce a system that is operative and meet the specifications as described in Claim 3.

Claim 4

The last O.A notes (p.10) that L. Brown's teaching describes the use of SOAP security extension, SSL and HTTP in IBM WebSphere Application Server 4.0. The last O.A. suggests that the combination of Martherus, Guski, and L. Brown's teaching would have been obvious.

The same reason explained in the remark of Claim 2 can be used to prove that Claim 4 is not obvious. It is improbable for Martherus's system to use SOAP over HTTP and SSL in the context of adopting Web services technology, because it requires a significant architecture change. Thus, the combination of referenced arts will not produce a system that is operative and meet the specifications as described in Claim 4.

Claim 5

The last O.A. notes (p.11) that L. Brown's teaching describes the transport of SOAP using IBM MQSeries, FTP, and mail messages. The last O.A. suggests that the combination of Martherus, Guski, and L. Brown's teaching would have been obvious.

The same reason explained in the remark of Claim 2 can be used to prove that Claim 5 is not obvious. It is improbable for Martherus's system to use SOAP over FTP and mail messages in the context of adopting Web services technology, because it requires a significant architecture change. Thus, the combination of referenced arts will not produce a system that is operative and meet the specifications as described in Claim 5.

CONCLUSION

For all the above reasons, applicants submit that the claims are now in proper form, and that the claims all define patentable over the prior art. Therefore, they submit that this application is now in condition for allowance, which action they respectfully solicit.

Conditional Request for Constructive Assistance

Applicants have amended the claims of this application so that they are proper, definite, and define novel structure which is also unobvious. If, for any reason this application is not believed to be in full condition for allowance, applicants respectfully request the constructive assistance and suggestions in order that this application can be placed in allowable condition as soon as possible and without the need for further proceedings.

Chaing Chen
8778 Boulder Ridge RD
Laurel, MD 20723-5901
Tel. (301) 617-4370